Optical Fiber Tapping: Methods and Precautions

M. Zafar Iqbal, Habib Fathallah, Nezih Belhadj

Abstract— **Optical fiber communication is not as secure as generally perceived. There are a number of known methods of extracting or injecting information into a fiber link, while avoiding detection. Few incidents have been reported as a successfully tapped fiber is difficult to detect. In this paper we highlight a number of known fiber tapping methods. We report simulation of optical characteristics of a fiber being tapped by 'bend' method and proof of concept with physical experiment. We also presented visualized scenarios in which a resourceful eavesdropper can compromise security of a fiber link with existing technologies. Some measures to prevent fiber tapping or to nullify the significance of information tapped from fiber were also discussed.**

***Index Terms*— Optical Fiber Tapping, Layer 2 Encryption Eavesdropping, Bend tapping.**

I. Introduction

CONTRARY to the common perception, optical fiber is not inherently secure from tapping or eavesdropping. The enormous amount of mission critical and sensitive information carried over fiber these days is exposed to any determined and resourceful eavesdropper.

Fiber tapping is a process by which the security of optical fiber is compromised by either extracting or injecting information (as light). Basically fiber tapping can be intrusive and non-intrusive. The former requires the fiber to be cut and reconnected into the tapping mechanism while the later achieves tapping without cutting the fiber or causing any service disruption. Non-intrusive technique is the focus of this work.

Only a few incidents of fiber tapping could be reported as it is very difficult to detect a tapped fiber while the tapping process itself is quite simple. Major reported incidents of tapping include the following:

- 2000, three main trunk lines of Deutsche Telekom were breached at Frankfurt Airport in Germany [1].
- 2003, an illegal eavesdropping device was discovered hooked into Verizon's optical network [1].
- 2005, USS Jimmy Carter, submarine specifically retrofitted to conduct tapping into undersea cables [2], [3].

In the following sections we present a brief overview of intrusive and nonintrusive tapping techniques [4]. Then we present a numerical simulation of signal loss due to fiber bending followed by a report on physical demonstration of tapping on a prototype developed in our lab. Here we also explain the prototype design, hardware and software. We also discuss possible tapping scenarios in real environments highlighting the resources required to achieve it. Finally we propose some solutions to protect optical fiber links against tapping.

This paper is based on work that was supported by the Royal Saudi Air force of Kingdom of Saudi Arabia.

M. Zafar Iqbal is working in Prince Sultan Advance Technologies Research Institute (ziqbal@ksu.edu.sa)

Habiab Fathallah is an Associate Professor at King Saud University (hfathallah@ksu.edi.sa)

Nezih Belhadj is a postdoctoral researcher at Laval University (nbelhadj@gel.ulaval.ca).

978-1-4577-1169-5/11/$26.00 ©2011 IEEE

II. Fiber Tapping Methods

A. *Fiber Bending*

In this method cable is stripped down to the fiber for bending. This method exploits the principle of propagation of light through an optical fiber better described as the total internal reflection. To achieve this, angle of incidence of light on the core cladding interface should be greater than the Critical Angle for total internal reflection. Otherwise some light will radiate out of the fiber through its cladding. The critical angle is a function of the refractive indices of the core and cladding, and represented by the following equation:

$$\theta c = Cos^{-1}(\mu_{cladding} / \mu_{core}) \qquad (provided\ \mu_{cl} < \mu_c)$$

Where, θc is the critical Angle, μ_{cl} is refractive index of Cladding, μ_c is refractive Index of Cladding

In fiber bending techniques the fiber is bent such that the angle of incidence becomes less than the critical angle and the light radiates. Apparently there are further two types of fiber bending:

1) *Micro Bending*

Application of external force results in sharp but microscopic curvatures resulting in axial displacements of a few microns and spatial wavelength displacements of a few millimeters (Figure 1). The light thus radiated is used for tapping.

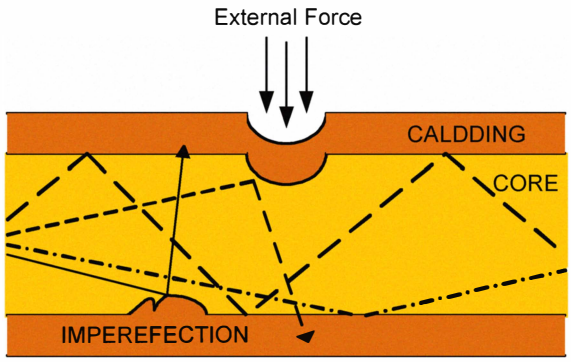

Figure 1 Micro Bending

2) *Macro Bending:*

There is a minimum tolerable bend radius associated with each fiber type. A lesser bend radius will result in radiation of Light (figure 2). This property can be used to extract light from fiber for eaves dropping. Normally, single mode fibers will not tolerate a minimum bend radius of less than 6.5 to 7.5 cm except some specially developed types. While a

multimode fiber can tolerate a bend radius as less as 3.8cm.

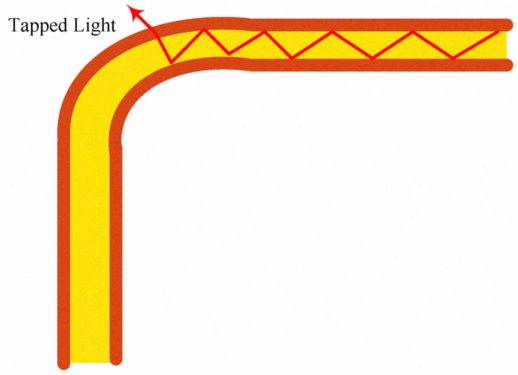

Figure 2. Macro Bending

B. *Optical Splitting*

The target fiber is inserted into a splitter to tap a part of the optical signal. But this method is intrusive as it involves cutting the fiber that raises alarms. However, an undetected tap of this type can work for years.

C. *Evanescent Coupling*

This involves capturing signal from the target fiber into the receiver fiber by polishing cladding of both to the edge of respective core and placing them together. This allows some signals to leak into the receiving fiber. However, this method is very difficult to implement under the field conditions.

D. *V Groove Cut*

A V-groove is a cut in the cladding of the fiber close to its core such that the angle between the light propagating in the fiber and the face of V-groove is greater than the critical angle. This causes total internal reflection where a fraction of the light that is travelling in the cladding and overlapping V-grove will leak out of the fiber.

E. *Scattering*

Bragg Grating is etched in the core of the fiber to achieve reflection of some signals out of the fiber. This is achieved by creating an overlapping and interfering rays of UV rays by UV Exciter laser.

III. Simulation

A. *Methodology:*

A full vectorial Maxwell solver in the frequency domain based on a High-Order Finit Element Method and allowing the adaptation of the stretching PML (Perfectly Matched Layer) technique is used to precisely estimate bending losses in an SMF-28 optical fibre. So, Vectorial computation of the propagation constants and the electric fields of the modes in bend waveguides is achieved. The bend losses are computed from the imaginary part of the propagation constant of the fundamental mode. The total losses are obtained by adding the losses of both orthogonal fundamental modes. The results obtained by this method are very accurate and have been validated in [5]

B. *Simulation Data:*

For the SMF-28 fiber, the core radius and refractive index are respectively:

$$r_c = 4.15\ \mu m \text{ and } n_c = 1.4493$$

Where in the cladding, they are respectively:

$$r_{cl} = 62.25\ \mu m \text{ and } n_{cl} = 1.444.$$

The refractive index of the air is 1.

The curvature radius ρ is along the x axis, the mode is polarized along the y axis and the propagation is along z axis as shown in Figure 3

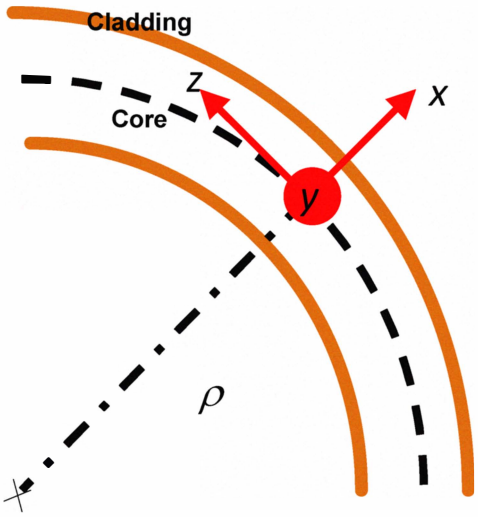

Figure 3

C. *Power Loss Computation:*

Figure 4 represents the numerical estimated bend loss as a function of the curvature radius for 1 meter bending fiber. A logarithmic dependence of losses versus curvature radius is observed. For smaller curvature radii ($\rho <$ 10mm), losses exceed 40 dB/m. For more usual values of curvature radius ($\rho >$ 15mm) the losses are less than 1 dB/m.

IV. Fiber Tapping Experiment

A. *Steps in Fiber Tapping*

The entire eavesdropping operation can be achieved in following steps:

i. Tapping optical signal from fiber.
ii. Detecting the signal.
iii. Detecting the Transmission Mechanism (Protocol).
iv. Software processing to detect the frames/ packets and extracting desired data from it.

The experiment involved transmitting a video over optical Ethernet from one computer to the other. The connecting fiber was stripped to cladding and pressed by a device called "Clip on Coupler" which basically bends the fiber inducing radiation of some light that violate principle of total internet reflection. This device directs this trapped light to a Unidirectional Ethernet media converter and eventually Ethernet frames are processed to reconstruct a copy of original video frames in a third PC. We used VLC for video streaming and playback. Wire-Shark Protocol Analyzer to capture packets and 'Chaosreader' to reconstruct video clippings from the captured packets.

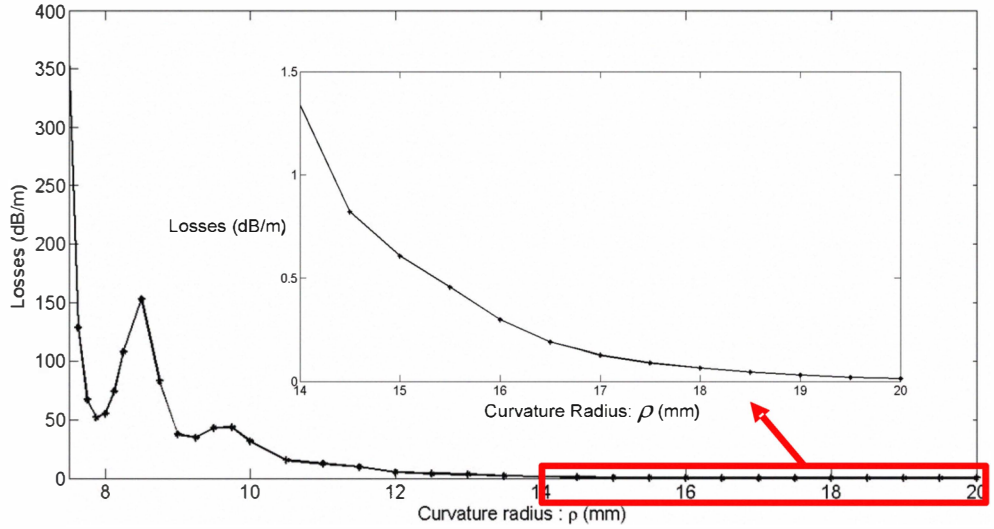

Figure 4. Numerical estimation of bend loss as a function of curvature radius

B. *Procedure*

Above mentioned hardware and software are connected as shown in figure 5. The stripped fiber strand in the direction from video source to destination is placed under the clamp of Clip-on-Coupler. The clamp is pressed resulting in some light feeding and exciting the unidirectional media converter which reads Ethernet frames and feeds the third PC equipped with Wire-Shark. Wire-Shark converts Ethernet frames and provides information such as source and destinations MAC addresses. It also processes Ethernet frame payload and obtains the IP packets from it. The information obtained from the packets includes IP addresses, signaling protocol messages and payload bits. The packets thus captured are saved in "pcap" (packet capture) format file. This file is then processed by software called "chaosreader" which reconstructs original files and creates an index of reconstructed files. For our captured video, we look in the index, for *.DAT file of large size. Opening this file in VLC software opens the captured portion of the video stream.

C. *Possible Eavesdropping Actions*

Besides Video Play back, the experimental setup describe here can be used to perform as number of eavesdropping operations such as Attacking IPs, password stealing, listening VoIP calls and email reconstructions using various free, commercial or self-developed software.

V. Further Tapping Scenarios

The experiment reported here was performed on an Ethernet network as the components especially the software were easily available. However, several real-world tapping scenarios can be imagined such as:

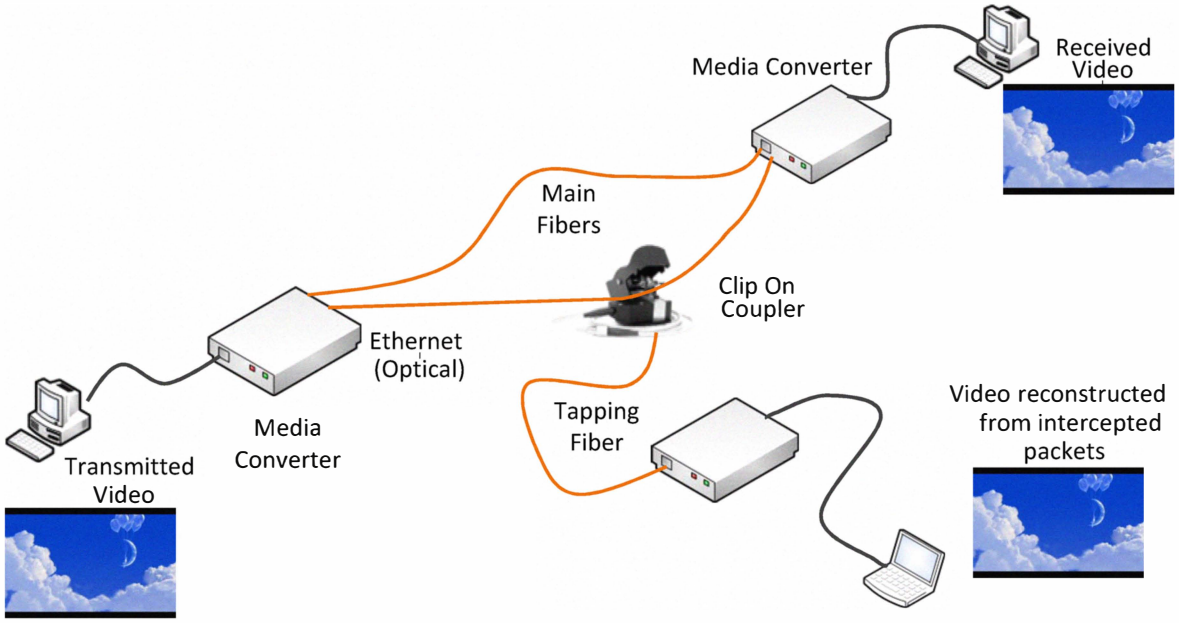

Figure 5.Experimental setup for bend tapping

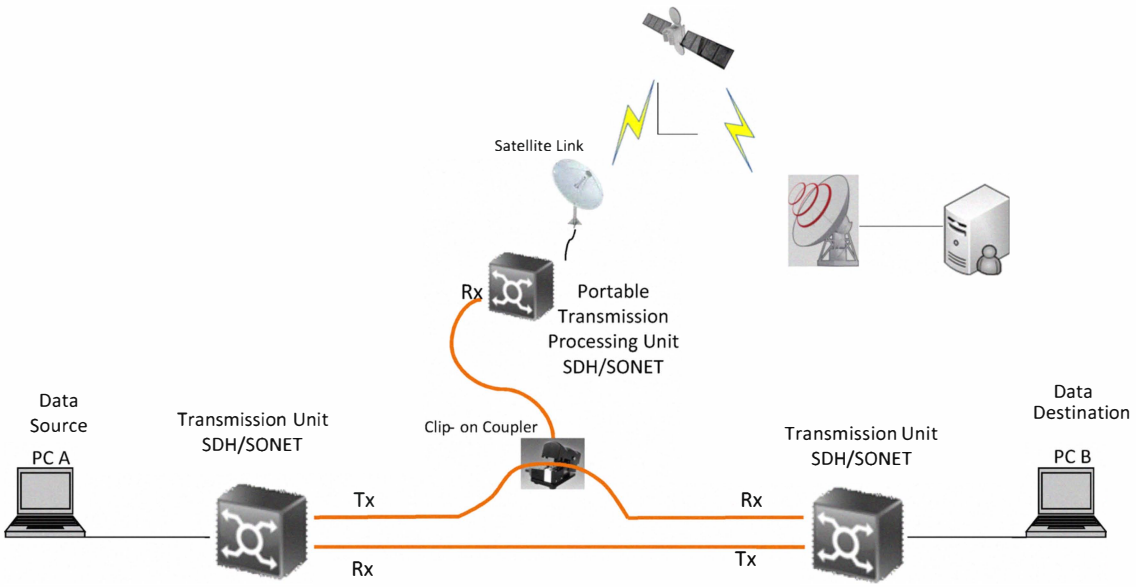

Figure 6 Tapping with Remote processing scenario

A. *Tapping Transmission Network*

Meaningful information can be obtained from transmission networks such as SDH and SONET, two most prevailing standards of optical fiber transmission over Long Haul and Metro networks. The very high speed data is difficult to be stored and processed but high-tech SDH protocol analyzers are available that can be used to obtain low level tributary signals [6]. This somewhat reduces the data rate complications. Such devices can be further developed to obtain various types of traffics flowing through the network. For example it may be able to extract an Ethernet stream mapped onto some VC4 container stream. Remotely Processed Tapping:

There are two important motivations for remote processing. (1) When tapping very-high bit-rate long haul transmission links of several Gbps, the role of storage capacity becomes important. This is due to the fact that the captured packet will quickly fill the hard disk. (2) Network Forensic experts may be too precious commodity to be deployed in the field. It is more desirable to have them at some remote processing location equipped with state of art resources which cannot be deployed in the field. Using imagination, some scenarios of remote processing of data tapped from a fiber can be easily conceived. For example:

1) Using Wireless Ethernet:

Using Wi-Fi, tapping laptop can be in another room or in a van outside the building where the tap is placed. The forensic expert can work in a position of relative safety with access to better resources.

2) Using Microwave/ Satellite Link:

Our experimental setup has been modified by Mapping Ethernet Traffic on a directional Microwave link (figure 6). The processing may be done tens or even thousands of kilometers away if Satellite link is used.

3) Signal Injection

By using the scattering method we described earlier, it is theoretically possible to construct a device that injects signals into a fiber using some sort of coupling technique. Sophisticated techniques can be developed to jam a fiber without breaking it or even injecting malicious information.

VI. PROTECTION AGAINST TAPPING

Three basic categories to prevent or nullify the impact of fiber tapping are considered in the following along with some discussion on respective subcategories.

A. *Cable Surveillance and Monitoring*

1) Monitoring Signals around the Fiber

Manufacture the optical cables with fibers surrounding them that carry only monitoring signals. Using this method will increase the cost of the cable but any attempt to bend the fiber will cause loss of monitoring signal which cable used to trigger alarms. [7].

2) Electrical Conductors:

Another method consists of integrating electrical conductors into the fiber cable transmitting the information. When the cable is tampered with, the capacitance between the electrical conductors is altered which can be used to trigger an alarm.

3) Modes' Power Monitoring

This applies to multimode fiber in which attenuation is a function of mode in which the light is being propagated. A tap affects certain modes resulting in all the other modes being affected. This leads to energy being redistributed from conducting to non-conducting modes and the power distribution in the fiber core and sheath are altered. This change in modes' power can be exploited in the receiver side by measuring the power contained in the modes and then decide if there is tapping or not [8].

4) Optical Mean Power Measuring

Fiber can be monitored by the optical mean power level being detected. An alarm signal being is triggered by change from a given reference value. This requires, however, that the optical signal is coded so that it has a constant mean power independent of its information content [8].

5) OTDRs

Since tapping involves extracting part of the optical signal, the Optical time domain reflect meters (OTDRs) can be used to detect if there is tapping by observing the locations within the fiber trace (figure 7.) that show decrease in signals power.[8]

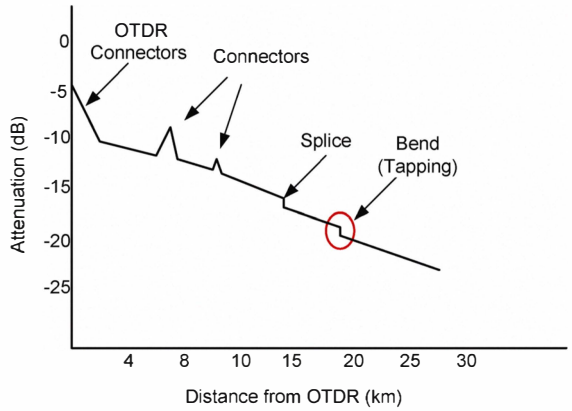

Figure 7 Finding Tap in OTDR trace

6) Pilot Tone Methods:

Pilot tones travel along the fiber as the communications data. They are used to detect transmission disruptions. Pilot tone methods can be used to detect jamming attacks. But, if the carrier wavelengths of pilot tones are not attacked, this method is not effective in detecting jamming attacks. Pilot tone method detects tapping attacks by determining whether the pilot tones on the tapped channel are affected or not. The pilot tones are affected if the tapping attack causes significant degradation of the signal [8].

B. *High Bend Fibers:*

These fibers, commonly referred to as low-loss high bend radius fibers, protect the network by limiting high losses that can result from fiber pinching or bending, therefore, making twisting, pulling and other physical manipulation of the fiber less damaging. There are several different designs based on various manufacturing techniques [9].

C. *Encryption*

Although encryption cannot prevent tapping it renders the stolen information useless by making it unintelligible for the eavesdropper. Encryption can be classified into Layer 2 and Layer 3 types.

1) Layer 3 Encryption

Example of Layer 2 encryption is IP Security Protocol which involves encryption of IP packets. It has to be implemented at end users thus causing processing delays. It has to be established at the beginning of session and overall implementation can be complicated if large number of network elements are involved. Consider for example the development of IP Multimedia Subsystem. In the initial development, communication between different nodes and elements was unsecured. It was only later that IPsec had to be coded into the original design as prevailing underlying transport technologies don't offer encryption.

2) Layer 2 Encryption

This type of encryption would free layer 3 entities from any burden of encrypting the information they are communicating. One possible source of Layer 2 encryption is Optical CDMA which is considered inherently secure [10-12]. This assumption is mostly based on only considering brute force deciphering methods, and overlooks other sophisticated methods. The probability of successful data interception is a function of several parameters, including signal-to-noise ratio and fraction of total available system capacity. In [12] it is shown that increasing code complexity can increase the signal-to-noise ratio (SNR) required for an eavesdropper to "break" the encoding by only a few dB, whereas the processing of fewer than 100 bits by an eavesdropper can reduce the SNR required to break the encoding by up to 12 dB. Time-spreading/wavelength-hopping in particular and O-CDMA in general, are found to provide confidentiality highly dependent on system design and implementation parameters.

ACKNOWLEDGMENT

The authors would like to thank Prince Sultan Advance Technology Research Institute for rendering its facilities to setup and perform experimental part of this work.

VII. CONCLUSION

Fiber Tapping is a tangible threat to the interests of national security, financial institutions or even personal privacy and freedoms. Once tapped, the information thus obtained can be used in many difference imaginative ways as per eavesdropper's motivations and resourcefulness. In this paper we proved the concept both in terms of simulation and physical experiment using 'bend tap' and also highlighted the possibility of a number of fiber tapping scenarios achievable using available technologies. Besides obtaining information from the fiber some techniques can be used to insert information into it, as in case of 'Evanescent splitting', and achieve link-jamming or feeding wrong information. The apparent ease of eavesdropping optical fiber warrants precautionary measures, also introduced in this paper.

REFERENCES

[1] Sandra Kay Miller, "Hacking at the Speed of Light", *Security Solutions Magazine*, April 2006

[2] Davis, USN, RADM John P."USS Jimmy Carter (SSN-23): Expanding Future SSN Missions". *Undersea Warfare*, Fall 1999 Vol. 2, No. 1

[3] Optical Illusion by: Sandra Kay Miller Information security Issue: Nov 2006.

[4] Optical Network Security: Technical Analysis of Fiber Tapping Mechanisms and Methods for detection and Prevention, Keith Shaneman & Dr. Stuart Gray, *IEEE Military Communications Conference* 2004.

[5] R. Jedidi and R. Pierre, High-Order Finite-Element Methods for the Computation of Bending Loss in Optical Waveguides, *JLT*, Vol. 25, No. 9, pp. 2618-30, SEP 2007.

[6] *FTB-8140 Transport Blazer - 40/43 Gigabit SONET/SDH Test Module*, EXFO

[7] "Optical Fiber Design for Secure Tap Proof transmission", *US Patent No. 6801700 B2*, Oct. 5, 2004.

[8] *All Optical Networks (AON)*, National Communication System, *NCS TIB 00-7, August 2000*

[9] *DrakaElite, BendBright-Elite Fiber for Patch Cord*, Draka Communications, July, 2010

[10] W. Ford, "*Computer Communications Security*", Upper Saddle River, NJ: Prentice-Hall, 1994.

[11] D. R. Stinson, "*Cryptography*", Boca Raton, FL: CRC, 1995.

[12] N. Ferguson and B. Schneier, "*Practical Cryptography*", Indianapolis, IN: Wiley, 2003.